

CLAIMS

What is claimed is:

1 1. A method of enforcing authorization in a shared process between at
 2 least two parties comprising:
 3 identifying a sender of a message requesting an action as part of the
 4 shared process;
 5 determining the party of the sender;
 6 associating the sender's party with a business relationship between the
 7 sender's party and the receiver's party as defined by an electronic contract,
 8 without relying on a trusted third party to provide a common rooted key hierarchy;
 9 identifying terms and conditions of the electronic contract corresponding
 10 to the shared process; and
 11 verifying that the requested action corresponds to the terms and
 12 conditions and is allowable for the shared process by the sender.

1 2. The method of claim 1, wherein verifying comprises at least one of
 2 using roles to determine that requested actions are sanctioned under the
 3 electronic contract, using digital certificates to determine processing systems
 4 implementing requested actions are authorized by the parties, and using public
 5 keys of the parties to verify adherence to the electronic contract.

1 3. The method of claim 1, wherein the electronic contract binds public
 2 keys for each of the parties with sub-processes of the shared process.

1 4. The method of claim 1, wherein at least a portion of the electronic
 2 contract is digitally signed by the at least two parties with their respective public
 3 keys prior to the sender sending the message.

1 5. The method of claim 1, wherein the shared process is defined by a
2 descriptive language.

1 6. The method of claim 1, wherein verifying comprises qualifying
2 semantics of security related decisions affecting the shared process using
3 information from the electronic contract.

1 7. An article comprising: a storage medium having a plurality of machine
2 readable instructions, wherein when the instructions are executed by a
3 processor, the instructions provide for enforcing authorization in a shared
4 process between at least two parties by identifying a sender of a message
5 requesting an action as part of the shared process, determining the party of the
6 sender, associating the sender's party with a business relationship between the
7 sender's party and the receiver's party as defined by an electronic contract,
8 without relying on a trusted third party to provide a common rooted key hierarchy,
9 identifying terms and conditions of the electronic contract corresponding to the
10 shared process, and verifying that the requested action corresponds to the terms
11 and conditions and is allowable for the shared process by the sender.

1 8. The article of claim 7, wherein the electronic contract binds public keys
2 for each of the parties with sub-processes of the shared process.

1 9. The article of claim 7, wherein the electronic contract is digitally signed
2 by the at least two parties with their respective public keys prior to the sender
3 sending the message.

1 10. An electronic contract associating at least two parties with a shared
2 process comprising:
3 a first section to specify at least one party, other than the at least two
4 parties, that represents a name space corresponding to a domain of
5 cryptographic keys;

6 a second section to associate the at least two parties liable under the
7 electronic contract with a public key of a cryptographic key pair from the domain
8 for each of the at least two parties, without relying on a trusted third party to
9 provide a common rooted key hierarchy;

10 a third section to provide at least one of mapping of role names and sub-
11 processes of the shared process; and

12 a fourth section to allow each of the at least two parties to digitally sign at
13 least a portion of the electronic contract with a private key of the cryptographic
14 key pair for each of the at least two parties.

15
1 11. The electronic contract of claim 10, further comprising a fifth section
2 to specify information identifying at least one of the electronic contract and
3 current revision level.

4
1 12. The electronic contract of claim 10, wherein the first section specifies
2 a security standard used for unambiguous references to process definitions,
3 protocols and names from which syntax and semantics of shared processes are
4 derived.

5
1 13. The electronic contract of claim 10, wherein the second section
2 comprises at least one of a contract identifier, validity period, creation date, and
3 contact information of the at least two parties.

4
1 14. The electronic contact of claim 10, wherein the third section
2 comprises information to specify syntax and semantics of role names.

3
1 15. The electronic contract of claim 10, further comprising a sixth section
2 defining ancillary services used in support of the shared process.

3

1 16. The electronic contract of claim 15, wherein the ancillary services
2 comprise saving archives relating to use of the shared process by the at least
3 two parties.

1 17. The electronic contract of claim 15, wherein the ancillary services
2 comprise performing audits relating to use of the shared process by the at least
3 two parties.

1 18. The electronic contract of claim 15, wherein the ancillary services
2 comprise timestamping the electronic contract.

1 19. The electronic contract of claim 15, wherein the sixth section specifies
2 a party, other than the at least two parties, that provides the ancillary services to
3 the at least two parties as part of the shared process.